TABLE OF CONTENTS

LIST OF FIGURES

SECTION 4
INFORMATION ASSURANCE

Information Assurance is a key aspect in the design of any Internet protocol (IP)-based network. Internet Protocol is inherently vulnerable to eavesdropping and a variety of denial of service (DoS) attacks. Voice and Video over IP (VVoIP) introduces avenues of attack because of its use of dynamically assigned User Datagram Protocol (UDP) sessions that cannot be addressed by traditional data firewalls. Therefore, VVoIP are applications that use IP for transport and inherit the threats associated with IP as well as adding vulnerabilities that are unique to the VVoIP technology. A tailored VVoIP information assurance design is necessary and is addressed in detail in Unified Capabilities Requirements (UCR) 2013 Section 4, Information Assurance DISA Field Security Office (FSO) Security Technical Implementation Guides (STIGs), and Security Requirements Guides (SRGs). With respect to the DoD UC architecture, the major components of the Information Assurance design include the protocols used, the interfaces of Session Controllers (SCs)/Enterprises SCs (ESCs) and Softswitch (SS) to external control devices, and the design of the Assured Services Local Area Network (LAN) (ASLAN). As an example, the methods for securing the VVoIP protocols are illustrated in Figure 4-1, Information Assurance Protocols. Key to the design is a hop-by-hop security model for trust between the signaling appliances using the Department of Defense (DoD) Public Key Infrastructure (PKI) for authentication. The diagrams illustrates an example of the UC distributed SC architecture however, the same protocols and concepts apply to the ESC architecture as well.

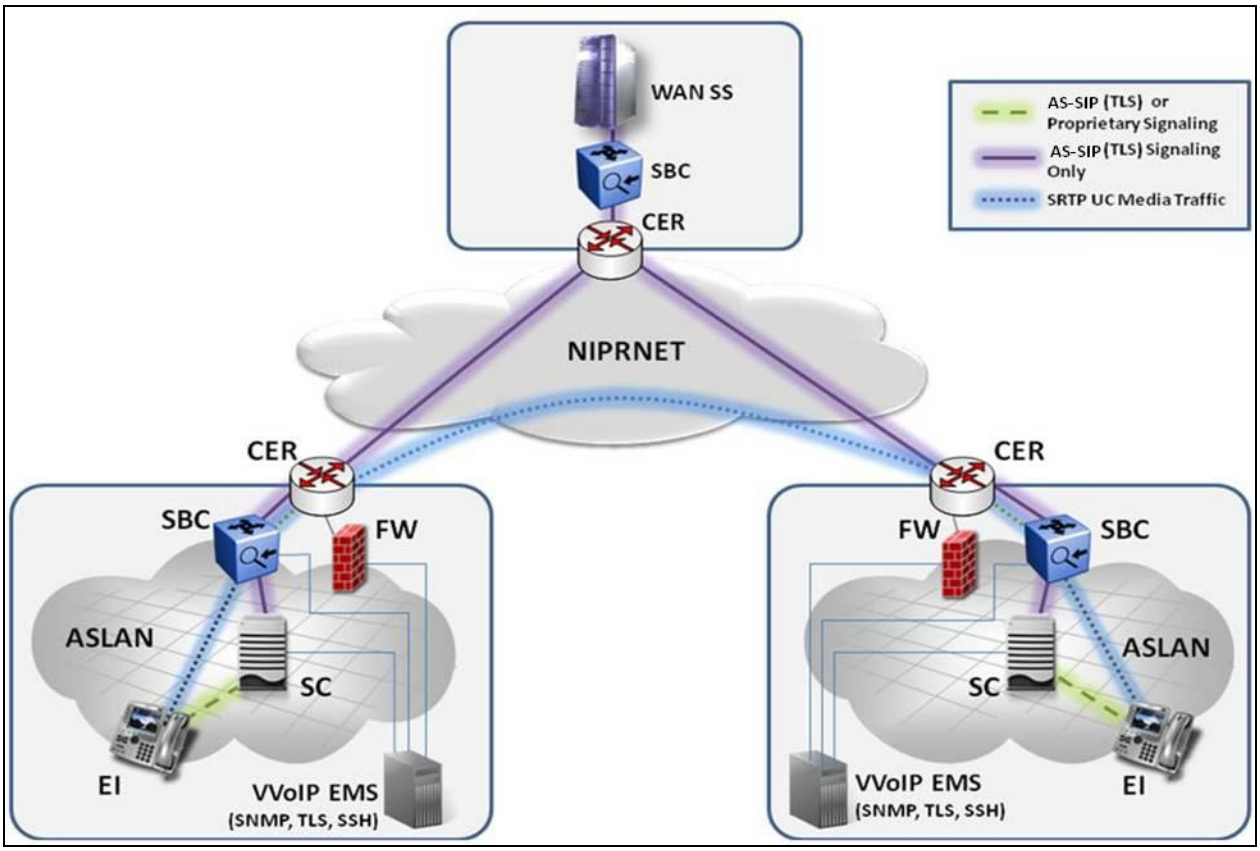

Figure 4-1. Example of Information Assurance Protocol Usage in the DoD UC Architecture

Figure 4-2, ASLAN Enclave Boundary Security Diagram, depicts a diagram of the Information Assurance design needed as part of the ASLAN. The key feature of Figure 4-2 is the need for two types of firewalls: one for data traffic and another for VVoIP traffic. The voice and/or video signaling packets and media stream packets must traverse the edge boundary control device that implements a voice and/or video dynamic stateful Assured Services (AS) Session Initiation Protocol (AS-SIP) aware application firewall, which provides Network Address Translation (NAT), SS failover, and port pinholes for individual voice and video sessions. A UC Approved Products List (APL) product called an SBC consisting of the voice and/or video firewall/border controller, has been defined and specified in UCR 2013, Section 7. In an Enterprise configuration, the site can be in a single Information Assurance accreditation boundary in which the SBCs shown in the diagram will be associated with the ARs and will not be within the Enclave Boundary shown on the diagram.

The requirements for the information assurance interoperability requirements are generally provided in UCR 2013, Section 4, Information Assurance. The result from testing against against these UCR requirements are adjudicated and placed in Interoperability (IO) Test Reports. The STIGs and SRGs provide the other basis for UC APL information assreance requirements and any findings against these requirements during testing are documented in IA Test Reports.

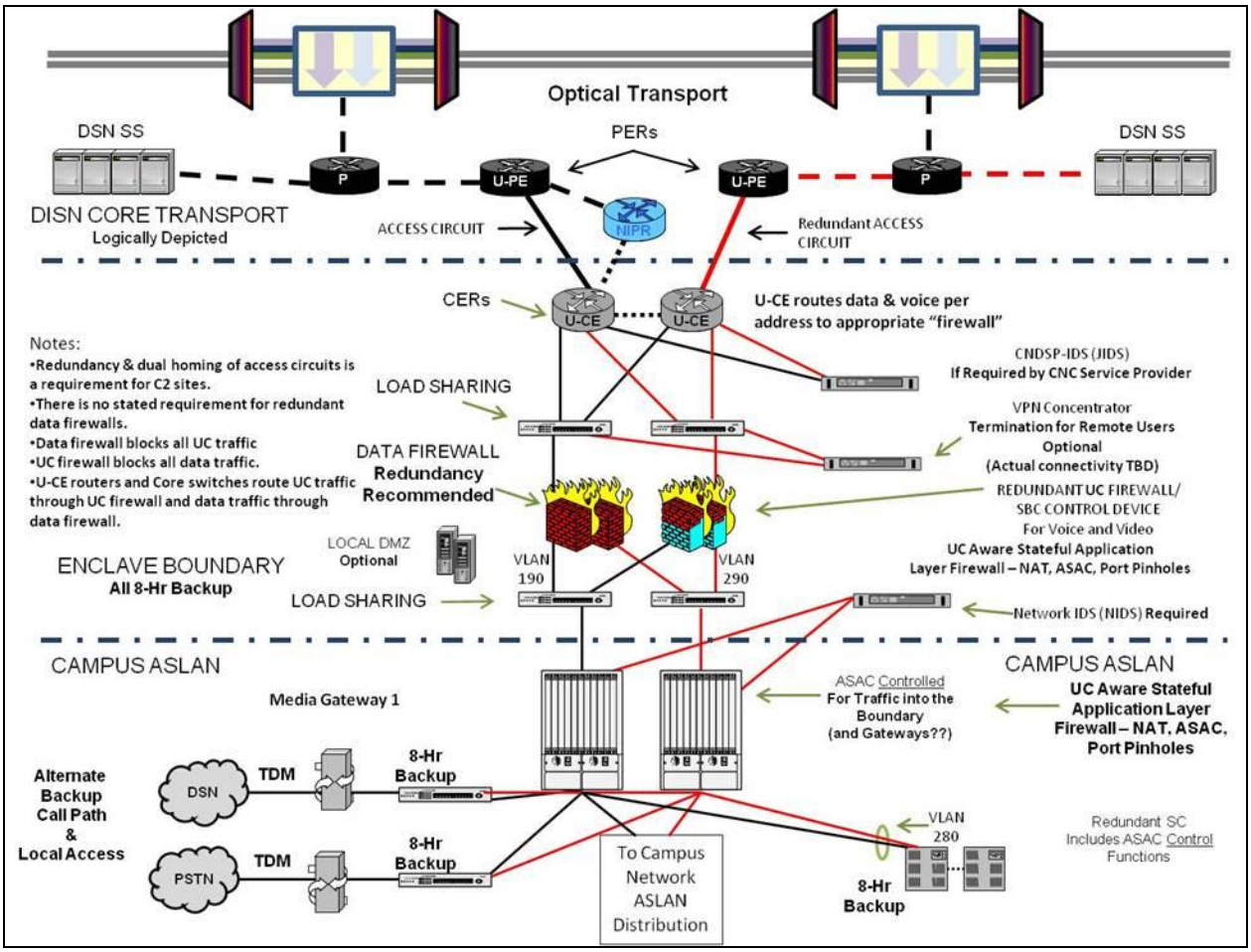

Figure 4-2. ASLAN Enclave Boundary Security Design